Office of the State Auditor

Kerri L. Hunter, CPA, CFE
State Auditor

December 5, 2025

A Request for Proposals for an IT Performance Audit of Information Security at the Colorado Community College System

Responses to Prospective Bidder Inquiries

Questions from Prospective Bidder #1:

1. We need to know if a penetration test is required to validate the security controls we will be auditing? If so, how many IP's/devices are in scope for the project?

   OSA Response: Please see "Section C" of the RFP for a description of the services required and the audit objectives, scope, and methodology. Within this section, there is no requirement for a penetration test for this audit, which must be performed under GAGAS. Thus, the second question part is not applicable.

Questions from Prospective Bidder #2:

2. Can you clarify the extent to which practices at individual colleges should be reviewed? Is it limited strictly to CCCS's oversight, or are there scenarios where direct evaluation of college-level controls is expected?

   OSA Response: The intent of this audit is to evaluate the system-level CCCS information security program and controls, not those at the individual colleges. Therefore, we do not anticipate any scenarios where direct evaluation of individual, college-level controls would be performed as a part of this audit.

3. Can you clarify the formal communication and reporting structure between CCCS and its community colleges regarding IT governance, security oversight, and compliance with statutory requirements?

   OSA Response: We are unaware of the specifics regarding the formal communication and reporting structure between CCCS and its community colleges regarding those aspects. Based on the services we are requesting, however, we would see these areas as being in scope to achieve the audit objectives. As such, once the engagement commences, the selected Contractor

would need to gain an understanding of those areas, assess the information during the Contractor's risk assessment procedures and when planning the work necessary to audit the related processes and controls, as applicable, in order to satisfy the audit objectives, project deliverables, and timelines, as outlined in the RFP.

Questions from Prospective Bidder #3:

4. Can CCCS provide a complete inventory of its information security program documents (policies, standards, procedures, guidelines)?

   OSA Response: Once the engagement commences, this information should be requested of CCCS, by the selected Contractor, to assess and utilize the information, as applicable, during its risk assessment procedures and when planning the audit work necessary to satisfy the objectives, project deliverables, and timelines, as outlined in the RFP. Please see "Section C" of the RFP for a description of the services required and the audit objectives, scope and methodology.

5. Are there separate documents for System-level controls vs. College-level supplemental controls?

   OSA Response: See OSA response to question 4.

6. How are responsibilities divided between System Office IT, System Information Security, and local College IT departments?

   OSA Response: See OSA response to question 4.

7. Are there any shared governance committees, working groups, or advisory councils?

   OSA Response: See OSA response to question 4.

8. Can CCCS provide organizational charts for System IT, Information Security, and College IT departments?

   OSA Response: See OSA response to question 4.

9. Which reporting group (1, 2, or 3) does CCCS belong to for mandatory submission under C.R.S. 24-37.5-404.5(3)(b)?

   OSA Response: See OSA response to question 4.

10. When was the most recent report submitted to CDHE and the State CISO?

    OSA Response: See OSA response to question 4.

11. What security tests has CCCS performed annually over the last 3 years (penetration tests, risk assessments, tabletop exercises)?

    OSA Response: See OSA response to question 4.

12. Does CCCS use third-party vendors for assessments?

    OSA Response: See OSA response to question 4.

13. What framework(s) are currently used for risk assessments (NIST CSF, 800-53, ISO 27001, internal model)?

    OSA Response: See OSA response to question 4.

14. Can CCCS provide a complete list of enterprise systems and applications supporting System-wide operations?

    OSA Response: See OSA response to question 4.

15. Which systems contain PII, FERPA, financial, or other sensitive data?

    OSA Response: See OSA response to question 4.

16. Are there priority systems CCCS wants the audit to focus on?

    OSA Response: See OSA response to question 4. Additionally, the contract for this audit will be with the OSA, not CCCS. As such, although CCCS may provide information related to which systems to prioritize for this audit, the Contractor will need to work with the OSA contract monitor, as noted in the RFP, to review and approve its proposed scope and methodology, prior to engaging in the fieldwork steps necessary to achieve the audit objective.

17. Are SaaS platforms included in the System's security program?

    OSA Response: See OSA response to question 4.

18. What identity and access management technologies are used (Azure AD, AD DS, SSO, MFA)?

    OSA Response: See OSA response to question 4.

19. Are IAM controls centrally enforced across colleges?

    OSA Response: See OSA response to question 4.

20. What is the current procedure for reporting incidents to CDHE and the State CISO?

    OSA Response: See OSA response to question 4.

21. How many incidents were reported over the last 3 years?

OSA Response: See OSA response to question 4.

22. Does CCCS maintain formalized IR playbooks?

OSA Response: See OSA response to question 4.

23. Are colleges required to follow System-level procedures during an incident?

OSA Response: See OSA response to question 4.

24. Are there separate BC/DR plans for System IT and each community college?

OSA Response: See OSA response to question 4.

25. When were these last tested (tabletop or live failover)?

OSA Response: See OSA response to question 4.

26. What are CCCS's defined "mission-critical" systems for continuity planning?

OSA Response: See OSA response to question 4.

27. Which security controls are System-mandated vs. college-discretionary?

OSA Response: See OSA response to question 4.

28. Do colleges perform their own risk assessments or rely solely on the System?

OSA Response: See OSA response to question 4.

29. Does the OSA expect sampling of ALL 13 colleges for governance alignment, or can a risk-based selection model be used?

OSA Response: See OSA response to question 2.

30. Will CCCS provide read-only access to systems or only documentary evidence?

OSA Response: The selected Contractor would need to assess whether such access would be necessary to achieve the audit objectives, project deliverables, and timelines, as outlined in the RFP. If deemed necessary for this purpose, the Contractor would need to work with CCCS, and the OSA contract monitor, if necessary, to request the access and have it provisioned accordingly.

31. Is remote access allowed for evidence review?

OSA Response: As noted in the RFP, on page ten, depending on the needs of the engagement or the nature of work being performed, some work for this engagement may be able to be completed using email, phone, and other virtual file-sharing and remote meeting technologies. However, some amount of in-person or on-site work at CCCS and its campuses may also be required. The Contractor will work directly with CCCS during the engagement, and the OSA contract monitor, if needed, to determine an appropriate work location necessary to complete the services requested and the various related work tasks to meet the audit objective.

32. Does CCCS use tools such as these, and are they available for us to leverage:

    1. SIEM (Splunk, Sentinel)
    2. Vulnerability scanning (Qualys, Tenable, Rapid7)
    3. Asset management tools
    4. GRC platforms?

OSA Response: See OSA response to question 4.

33. Will site visits be required for multiple CCCS campuses?

OSA Response: See OSA response to questions 2 and 31.

34. If yes, which campuses are considered "primary" for IT operations?

OSA Response: See OSA response to questions 2, 4, and 31.

35. Are interviews required with college-level IT/security teams or only System-level staff?

OSA Response: See OSA response to questions 2 and 4.

36. Does the audit include any physical security controls of datacenters or campus facilities?

OSA Response: The audit scope will include those System-wide and/or campus IT and information security governance structures, policies, standards, procedures, and practices that are overseen and managed by CCCS. Therefore, the Contractor will need to gain an understanding of CCCS's information security governance and operations, including any related to physical security, in order to plan and develop a detailed, risk-based project scope and methodology, that will be reviewed and approved by the OSA, prior to engaging in the fieldwork steps necessary to achieve the audit objective.

37. How often does the OSA expect interim findings or fieldwork updates?

OSA Response: As noted on page 11 of the RFP, project updates, including any interim findings or fieldwork updates, are to be provided ongoing regularly (e.g., bi-weekly, etc.) through the completion of the contract as necessary, starting approximately the week of 3/9/2026. More immediate, ad hoc update communications may also be necessary for any urgent or pressing issues, typically those which may impact the achievement of the audit objective or project timelines.

38. Will OSA participate in testing design reviews or only approve the initial roadmap?

OSA Response: Although the Contractor's work is subject to oversight and direction provided by the OSA, the Contractor will be responsible for planning and conducting the audit, including any testing of design reviews, to obtain sufficient, appropriate evidence necessary to conclude on the audit's objectives and develop complete written findings, as applicable. The Contractor will work with the OSA to review and approve its proposed scope and methodology, prior to engaging in the fieldwork steps necessary to achieve the audit objective.

39. Will the OSA provide templates for Exhibit G (Findings) and Exhibit H (Report)?

OSA Response: The findings must adhere to the OSA's standards as described in "Exhibit G–Developing and Presenting Findings" of the OSA's standard contract. The final report must adhere to the OSA's standards as described in "Exhibit H–Reporting Requirements and Format for Separately Issued Reports" of the OSA's standard contract. The OSA's standard contract containing both exhibits is included in the RFP, in Section IV–Supplemental Information. If the Contractor needs templates for the findings and report beyond that which is shown in Exhibits H and G of the OSA's standard contract, this should be discussed with the OSA contract monitor.

40. Does the OSA expect the Contractor to independently determine which content goes into the confidential vs. public report?

OSA Response: As noted in the RFP on page 13, "The State Auditor and contract monitor will assist in making this determination."

41. Are there historical examples of similar confidential reports we can reference?

OSA Response: This would be a possibility. However, any such prior historical examples of confidential reports containing sensitive information would need to be cleansed and redacted to protect state resources and information and to ensure compliance with Colorado Revised Statutes.

42. Are there any data sources we will not have access to due to FERPA or confidentiality restrictions?

OSA Response: The State Auditor is authorized to access all accounts, records, or other data, including confidential data that are required to complete an audit.

According to Section 2-3-107(2)(a), C.R.S., the State Auditor or designated representative "shall have access at all times…to all of the books, accounts, reports, vouchers, or other records or information in any department, institution, or agency." This right of access includes "records or information required to be kept confidential or exempt from public disclosure upon subpoena, search warrant, discovery proceedings, or otherwise." When accessing confidential health records, statute requires the State Auditor to determine whether the information is necessary to achieve the audit objectives. However, the Contractor should involve the OSA contract monitor promptly if any issues arise related to CCCS restricting access to information necessary to complete the audit objectives.

43. Is CCCS undergoing any major IT initiatives (ERP migration, cybersecurity upgrades, cloud migration, etc.) during 2026 that may impact audit timelines?

OSA Response: See OSA response to question 4.

44. Who will be CCCS's primary coordinator?

OSA Response: We have obtained initial contact information for an individual at CCCS who will serve as the primary point of contact, or audit liaison, for this engagement. This information will be provided to the selected contractor once the contract is awarded.

45. Will there be dedicated resources to respond to audit requests?

OSA Response: CCCS management is responsible for making available to the auditor all records, agency personnel, and related information required for the audit. As such, although the Contractor will be responsible for working with CCCS to ensure that this occurs in a timely manner, the Contractor should involve the OSA contract monitor promptly if any related issues arise in this area that might adversely impact its ability to conduct the audit to meet the overall audit objectives and project timelines as prescribed.

46. What is the expected SLA for CCCS responses to document requests?

OSA Response: The Contractor will be responsible for working with CCCS to ensure that CCCS document requests are fulfilled within reasonable deadlines to, ultimately, meet overall project deadlines. Also, see OSA response to question 45.

47. Can CCCS or OSA share any previous IT audits or cybersecurity assessments that would help in scoping?

OSA Response: This would be a possibility, if available. See OSA response to question 4.

48. Are there outstanding cybersecurity initiatives tied to previous recommendations?

OSA Response: We are not aware of any. However, once the engagement commences, this information should be requested of CCCS, by the selected Contractor, to assess and utilize the information, as applicable, during its risk assessment procedures and when planning the audit work necessary to satisfy the objectives, project deliverables, and timelines, as outlined in the RFP.